THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF APPEALS

In Re Application of:		)
		) ATTORNEY FILE NO.:
Inventors:	Sridhar Dathathraya	) SLA1055
		)
Serial No.:	09/944,695	)
		) Examiner: Ha, Leynna
		)
Filed:	August 31, 2001	) Customer No.: 55,286
		)
Title:	SYSTEM AND METHOD FOR SECURE COMMUNICATIONS WITH NETWORK PRINTERS	) Group Art: 2135)) Confirmation No.: 2135

CERTIFICATION UNDER 37 CFR § 1.8

I hereby certify that this correspondence is being facsimile transmitted to the US Patent and Trademark Office, fax No. 571 273 8300, on this date 1/19/2006.

Date 1/19/2006 Signature

Hon. Commissioner Of Patents And Trademarks
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

REPLY BRIEF ON APPEAL

This is a Reply Brief responsive to an Examiner's Answer dated December 30, 2005. At issue is the rejection by Examiner Leynna Ha, Group Art Unit 2135, of claims 1-8, 10-25, and 27-35, all claims in the application.

In addressing the rejection of claim 12, the Examiner states on page 6 of the *Examiner's Answer* that Mazzagatte and DeBry use symmetric and asymmetric algorithms interchangeably, and that "it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction." The Applicant respectfully submits that this answer neither provides any motivation to combine the two prior art references, nor correctly recites the key limitations of the claimed invention. The novelty of claim 12 does not necessarily stem from the type of encryption used, but rather from the fact the document is stored in an encrypted form at the printer, and that only the user has possession of the key that can decrypt (and print) the document.

Mazzagatte states that a document is sent from a sending node in either a secure transmission format (i.e., SSL), which only protects the document during transmission, or in a non-secure transmission format. If a non-secure transmission format is used, then the sending node encrypts the document before sending. Upon receiving the document, the first step performed by the printer is to decrypt the document (col. 8, ln. 5-18). Later in the process, the printer uses a symmetric (or asymmetric) key to store the document either locally or remotely (col. 9, ln. 7-24). However, the encryption key used is associated with either the printer or a gateway. None of these processes describe the claimed invention process, which protects the security of the user, not the security of a printer, a server, or a third party. Only the claimed invention process decrypts and prints a document in response to the user's key.

DeBry describes the use of encryption to protect the file source (i.e., a third party). Thus, even if DeBry is combined with Mazzagatte, the combination does not suggest that Mazzagatte be modified in such a manner as to give the user control of the document decryption key.

The limitations recited in claims 1, 19, and 29, are similar to limitations of claim 12, and these claims can likewise be distinguished from the Mazzagatte and DeBry references for the above-mentioned reasons.

It is submitted that the claims in the present application clearly and patentably distinguish over the cited references. Accordingly, the Examiner should be reversed and ordered to pass the case to issue.

Respectfully submitted,

Date: 1/19/2006

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net